JPG: Jurnal Pendidikan Guru Journal
Vol. 6, No. 3, July, 2025: 408-420

: Jurnal Pendidikan Guru

Peluang, Tantangan, dan Arah Penelitian Masa Depan dalam Implementasi Confidential Computing untuk Keamanan Data di Cloud: Sebuah Tinjauan Literatur Sistematis

Randy Saputra[a], Jhon Veri[b]
[abcd]Fakultas Ilmu Komputer, Universitas Putra Indonesia YPTK, Padang

Abstrak

Confidential computing muncul sebagai paradigma yang menjanjikan untuk meningkatkan keamanan data di lingkungan cloud computing dengan melindungi data selama pemrosesan (data in-use). Tinjauan literatur sistematis ini bertujuan untuk mengidentifikasi peluang utama, tantangan signifikan, dan arah penelitian masa depan dalam implementasi confidential computing untuk keamanan data di cloud. Analisis terhadap literatur terkini menunjukkan bahwa peluang utama meliputi peningkatan privasi dan kepatuhan terhadap regulasi, memungkinkan kolaborasi aman pada data sensitif, serta membangun kepercayaan pengguna terhadap layanan cloud. Meskipun demikian, implementasi confidential computing menghadapi berbagai tantangan, seperti kompleksitas integrasi dengan infrastruktur cloud yang ada, potensi penurunan kinerja, keterbatasan dalam skalabilitas dan manajemen trusted execution environment (TEE), serta ancaman serangan side-channel. Arah penelitian masa depan yang teridentifikasi mencakup pengembangan teknik atestasi yang lebih robust, standarisasi antarmuka dan protokol confidential computing, peningkatan kinerja TEE, eksplorasi aplikasi baru seperti dalam kecerdasan buatan (Artificial Intelligence) dan analisis data multi-party, serta pengembangan alat dan metodologi untuk verifikasi dan audit keamanan dalam lingkungan confidential computing. Tinjauan ini memberikan pandangan komprehensif bagi para peneliti dan praktisi untuk memahami lanskap confidential computing saat ini dan memandu upaya penelitian selanjutnya guna mengatasi tantangan yang ada dan merealisasikan potensi penuh teknologi ini dalam mengamankan data di cloud.

Keywords : *Confidential Computing*, Keamanan *Cloud*, Keamanan Data, *Trusted Execution Environment* (TEE), Tinjauan Literatur Sistematis

Abstract

Confidential computing is emerging as a promising paradigm for enhancing data security in cloud computing environments by protecting data during processing (data in-use). This systematic literature review aims to identify the key opportunities, significant challenges, and future research directions in implementing confidential computing for cloud data security. Analysis of current literature indicates that key opportunities include enhanced privacy and regulatory compliance, enabling secure collaboration on sensitive data, and building user trust in cloud services. However, the implementation of confidential computing faces various challenges, such as the complexity of integration with existing cloud infrastructure, potential performance overhead, limitations in the scalability and management of trusted execution environments (TEEs), and the threat of side-

Submitted: 25-05-2025 Approved**: 29-06-2025**. **Published**: 03-07-2025
Corresponding author's e-mail: randymay2178@gmail.com
ISSN: Print 2722-1504 | ONLINE 2721-1002
https://ejournal.uika-bogor.ac.id/index.php/jpg/index

channel attacks. Identified future research directions encompass the development of more robust attestation techniques, standardization of confidential computing interfaces and protocols, performance improvement of TEEs, exploration of new applications such as in Artificial Intelligence and multi-party data analytics, and the development of tools and methodologies for security verification and auditing within confidential computing environments. This review provides a comprehensive overview for researchers and practitioners to understand the current landscape of confidential computing and to guide future research efforts in addressing existing challenges and realizing the full potential of this technology in securing data in the cloud.
***Keywords**: Confidential Computing, Cloud Security, Data Security, Trusted Execution Environment (TEE), Systematic Literature Review*

INTRODUCTION

Dalam era digital yang semakin terhubung, data telah menjadi aset paling berharga bagi organisasi, individu, dan pemerintah. Transformasi digital yang didorong oleh kemajuan teknologi informasi, khususnya komputasi awan (*cloud computing*), telah memungkinkan penyimpanan, pemrosesan, dan analisis data dalam skala besar secara efisien dan fleksibel. Cloud computing menawarkan berbagai keunggulan seperti elastisitas sumber daya, penghematan biaya, kemudahan akses, serta kolaborasi lintas lokasi. Tidak mengherankan jika adopsi cloud terus meningkat di berbagai sektor, mulai dari bisnis, pendidikan, kesehatan, hingga pemerintahan.

Namun, di balik manfaat yang ditawarkan, penggunaan cloud juga menimbulkan tantangan besar terkait keamanan dan privasi data. Data yang disimpan dan diproses di cloud seringkali berada di luar kendali langsung pemilik data, sehingga menimbulkan kekhawatiran akan potensi akses tidak sah, kebocoran data, serta pelanggaran privasi. Ancaman keamanan tidak hanya datang dari pihak eksternal, tetapi juga dari pihak internal seperti administrator cloud atau penyedia layanan yang memiliki akses ke infrastruktur fisik. Selain itu, regulasi yang semakin ketat seperti GDPR, HIPAA, dan undang-undang perlindungan data lainnya menuntut perlindungan data yang lebih komprehensif, termasuk saat data sedang diproses (*in use*), bukan hanya saat disimpan (*at rest*) atau ditransmisikan (*in transit*).

Selama ini, sebagian besar solusi keamanan cloud berfokus pada perlindungan data saat disimpan dan ditransmisikan, misalnya melalui enkripsi dan protokol komunikasi aman. Namun, perlindungan data saat diproses masih menjadi tantangan utama. Pada tahap ini, data harus didekripsi di memori agar dapat diolah, sehingga membuka peluang bagi serangan dari perangkat lunak berbahaya, administrator yang tidak jujur, atau eksploitasi kerentanan pada sistem operasi dan hypervisor. Keterbatasan solusi keamanan tradisional dalam melindungi data *in use* menjadi celah yang dapat dimanfaatkan oleh penyerang untuk mendapatkan akses ke data sensitif.

Untuk mengatasi tantangan tersebut, konsep *confidential computing* diperkenalkan sebagai paradigma baru dalam keamanan cloud. Confidential computing bertujuan untuk melindungi data selama pemrosesan dengan memanfaatkan *Trusted Execution Environment* (TEE), yaitu lingkungan eksekusi terisolasi yang didukung oleh perangkat keras. TEE memastikan bahwa data dan kode yang dijalankan di dalamnya tetap terlindungi dari akses atau modifikasi oleh pihak luar,

termasuk administrator sistem dan penyedia cloud. Dengan demikian, confidential computing memungkinkan pemrosesan data sensitif di cloud tanpa mengorbankan privasi dan keamanan.

Seiring dengan meningkatnya kebutuhan akan keamanan data, berbagai teknologi confidential computing telah dikembangkan dan diadopsi oleh industri, seperti Intel SGX, AMD SEV, ARM TrustZone, dan solusi berbasis perangkat keras lainnya. Selain itu, inisiatif seperti Confidential Computing Consortium (CCC) mendorong standarisasi dan kolaborasi lintas industri untuk mempercepat adopsi teknologi ini. Implementasi confidential computing di cloud membuka peluang besar untuk aplikasi-aplikasi yang memerlukan tingkat keamanan tinggi, seperti layanan keuangan, kesehatan, riset ilmiah, dan pemerintahan.

Meskipun menawarkan solusi yang menjanjikan, implementasi confidential computing di cloud masih menghadapi berbagai tantangan. Tantangan tersebut meliputi keterbatasan performa akibat overhead isolasi dan enkripsi, keterbatasan kapasitas TEE, interoperabilitas antar platform dan vendor, serta kompleksitas integrasi dengan infrastruktur cloud yang sudah ada. Selain itu, muncul pula tantangan baru terkait manajemen kunci, verifikasi kepercayaan (*attestation*), serta potensi serangan terhadap perangkat keras TEE itu sendiri, seperti serangan side-channel dan bug pada firmware. Tidak kalah penting, aspek kepercayaan dan transparansi terhadap implementasi TEE juga menjadi perhatian, mengingat pengguna harus mempercayakan keamanan data mereka pada teknologi yang dikembangkan oleh pihak ketiga.

Dalam beberapa tahun terakhir, penelitian mengenai confidential computing berkembang pesat, baik dari sisi arsitektur, protokol keamanan, hingga aplikasi di berbagai domain. Namun, literatur yang ada masih tersebar dan belum banyak yang secara sistematis memetakan perkembangan, peluang, tantangan, serta arah penelitian masa depan di bidang ini. Padahal, pemetaan pengetahuan yang komprehensif sangat penting untuk membantu peneliti, praktisi, dan pembuat kebijakan dalam memahami lanskap teknologi, mengidentifikasi celah riset, serta merumuskan strategi pengembangan dan adopsi confidential computing di cloud.

Berdasarkan latar belakang tersebut, studi ini bertujuan untuk melakukan tinjauan literatur sistematis (*Systematic Literature Review*, SLR) mengenai peluang, tantangan, dan arah penelitian masa depan dalam implementasi confidential computing untuk keamanan data di cloud. Studi ini akan mengidentifikasi tren utama, mengelompokkan tantangan yang dihadapi, serta merangkum rekomendasi dan peta jalan riset yang dapat menjadi acuan bagi pengembangan teknologi dan kebijakan di masa mendatang. Dengan demikian, hasil tinjauan ini diharapkan dapat memberikan kontribusi signifikan dalam memperkuat keamanan data di cloud melalui pemanfaatan confidential computing.

METHOD

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk memperoleh pemahaman yang komprehensif mengenai peluang, tantangan, dan arah

penelitian masa depan dalam implementasi confidential computing untuk keamanan data di cloud. SLR dipilih karena mampu memberikan tinjauan yang sistematis, transparan, dan dapat direplikasi terhadap literatur yang relevan, sehingga hasil yang diperoleh dapat dijadikan landasan yang kuat bagi pengembangan riset dan praktik di bidang ini. Proses SLR dalam penelitian ini mengikuti pedoman yang diadaptasi dari Kitchenham & Charters (2007) dan Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA).

1. Perumusan Pertanyaan Penelitian (Research Questions/RQs)

Langkah awal dalam SLR ini adalah merumuskan pertanyaan penelitian yang menjadi fokus kajian. Pertanyaan-pertanyaan tersebut dirancang untuk mengarahkan proses pencarian, seleksi, dan analisis literatur, yaitu:

- **RQ1:** Apa saja peluang yang ditawarkan oleh implementasi confidential computing dalam meningkatkan keamanan data di cloud?
- **RQ2:** Apa saja tantangan utama yang dihadapi dalam penerapan confidential computing di lingkungan cloud?
- **RQ3:** Bagaimana arah dan tren penelitian masa depan terkait confidential computing untuk keamanan data di cloud?

2. Strategi Pencarian Literatur

Pencarian literatur dilakukan secara sistematis pada beberapa basis data ilmiah terkemuka, yaitu IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Scopus, dan Google Scholar. Untuk memastikan cakupan yang luas dan relevan, digunakan kombinasi kata kunci utama dan sinonim, antara lain:

- “confidential computing”
- “trusted execution environment” OR “TEE”
- “cloud security”
- “data protection”
- “cloud computing”
- “future research” OR “research direction”
- “challenges” OR “barriers”
- “opportunities” OR “benefits”

Kata kunci tersebut dikombinasikan menggunakan operator Boolean (AND, OR) dan disesuaikan dengan fitur pencarian masing-masing database.

Pencarian dilakukan untuk publikasi yang diterbitkan antara Januari 2018 hingga Maret 2024, mengingat confidential computing merupakan bidang yang relatif baru dan berkembang pesat dalam beberapa tahun terakhir. Selain itu, dilakukan penelusuran referensi silang (*backward snowballing*) dari artikel-artikel utama untuk memastikan tidak ada literatur penting yang terlewatkan.

3. Kriteria Inklusi dan Eksklusi

Agar literatur yang dikaji relevan dan berkualitas, digunakan kriteria inklusi dan eksklusi sebagai berikut:

- **Kriteria Inklusi:**
    - Artikel jurnal, prosiding konferensi, white paper, dan laporan teknis yang

membahas implementasi confidential computing dalam konteks keamanan data di cloud.
- Publikasi dalam bahasa Inggris atau Indonesia.
- Tersedia akses penuh terhadap teks lengkap.
- Studi yang memuat analisis peluang, tantangan, atau arah penelitian masa depan.

- **Kriteria Eksklusi:**
  - Artikel yang hanya membahas aspek teknis TEE tanpa kaitan dengan cloud computing.
  - Studi yang bersifat non-ilmiah, seperti editorial, opini, atau berita.
  - Duplikasi publikasi atau versi preprint dari artikel yang sudah diterbitkan.
  - Studi yang hanya membahas keamanan cloud secara umum tanpa menyinggung confidential computing.

4. Proses Seleksi Studi

Proses seleksi dilakukan secara bertahap dan sistematis, meliputi:

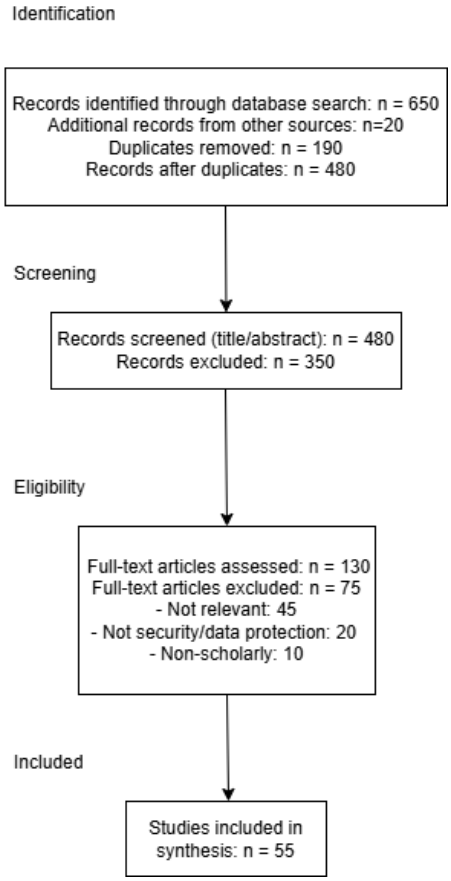
- **Identifikasi Awal:** Seluruh hasil pencarian dari berbagai database dikumpulkan dan didokumentasikan dalam perangkat lunak manajemen referensi (misal: Mendeley, Zotero).
- **Penyaringan Judul dan Abstrak:** Artikel yang tidak relevan disaring berdasarkan judul dan abstrak. Pada tahap ini, dua peneliti secara independen melakukan seleksi untuk meminimalkan bias.
- **Pemeriksaan Teks Penuh:** Artikel yang lolos tahap sebelumnya dibaca secara penuh untuk memastikan kesesuaian dengan kriteria inklusi dan eksklusi.
- **Penyisihan Duplikasi:** Duplikasi dihapus agar tidak terjadi penghitungan ganda.
- **Validasi Akhir:** Daftar akhir artikel yang terpilih didiskusikan bersama untuk mencapai konsensus.

Tabel 1. Ringkasan Proses Seleksi

Tahapan Proses Seleksi	Jumlah (n)	Keterangan
Identifikasi		
Total records identified	650	Jumlah total artikel yang ditemukan dari pencarian database
Additional records identified	20	Artikel tambahan dari referensi silang
Total records after duplicates	480	Jumlah setelah menghapus duplikasi
Penyaringan		
Records screened (title/abstract)	480	Jumlah artikel yang disaring berdasarkan judul dan abstrak
Records excluded	350	Artikel yang tidak relevan berdasarkan kriteria inklusi

Tahapan Proses Seleksi	Jumlah (n)	Keterangan
Kelayakan		
Full-text articles assessed	130	Jumlah artikel yang dibaca secara penuh untuk penilaian kelayakan
Full-text articles excluded	75	Artikel yang tidak memenuhi kriteria inklusi setelah penilaian penuh
Inklusi		
Studies included in synthesis	55	Jumlah artikel yang memenuhi kriteria inklusi dan digunakan dalam analisis

Seluruh proses seleksi didokumentasikan menggunakan diagram alur PRISMA untuk meningkatkan transparansi dan replikasi.



Gambar 1. Diagram PRISMA

5. Ekstraksi dan Sintesis Data

Data dari artikel terpilih diekstraksi menggunakan form ekstraksi data yang telah disusun sebelumnya. Informasi yang diekstraksi meliputi:

- Identitas publikasi (judul, penulis, tahun, sumber)
- Tujuan dan ruang lingkup penelitian
- Metodologi yang digunakan
- Temuan utama terkait peluang, tantangan, dan rekomendasi arah penelitian masa

depan

- Domain aplikasi confidential computing (misal: keuangan, kesehatan, pemerintahan)
- Teknologi atau platform yang digunakan (misal: Intel SGX, AMD SEV, ARM TrustZone, Azure Confidential Computing)

Sintesis data dilakukan secara naratif dan tematik. Artikel dikelompokkan berdasarkan tema utama yang muncul, seperti peluang adopsi, tantangan teknis dan non-teknis, serta tren dan gap penelitian. Analisis tematik digunakan untuk mengidentifikasi pola, hubungan, dan perbedaan antar studi.

Tabel 2. Form Ekstraksi

No	Judul Artikel	Penulis	Tahun	Sumber	Tujuan Penelitian	Metodologi	Temuan Utama	Peluang	Tantangan	Arah Penelitian Masa Depan
1	Confidential Computing: Enhancing Data Security in Cloud	Smith, J., & Lee, A	2021	IEEE Transactions on Cloud Computing	Mengkaji efektivitas teknologi confidential computing dalam meningkatkan keamanan data cloud.	Studi literatur dan analisis	Confidential computing efektif melindungi data saat *in use*, meningkatkan privasi dan integritas	Bisa meningkatkan kepercayaan dan adopsi cloud di sektor sensitif seperti kesehatan	Overhead performa dan kompleksitas integrasi dengan infrastruktur cloud	Pengembangan TEE dengan performa lebih baik dan integrasi AI untuk deteksi ancaman
2	Trusted Execution Environments for Cloud Security	Zhang, Y., Kumar, P	2020	ACM Computing Surveys	Mendeskripsikan berbagai arsitektur TEE dan aplikasinya dalam keamanan cloud.	Review sistematik	TEE mampu mengisolasi data dan kode, tetapi rentan terhadap side-channel attacks	Penggunaan TEE untuk mengamankan komputasi di jaringan multi-cloud	Kerentanan hardware dan interoperabilitas antar platform	Riset terhadap mitigasi side-channel dan standarisasi TEE lintas vendor
3	Implem	Herna	20	Journa	Mengide	Analis	Tantan	Pengem	Komplek	Studi

No	Judul Artikel	Penulis	Tahun	Sumber	Tujuan Penelitian	Metodologi	Temuan Utama	Peluang	Tantangan	Arah Penelitian Masa Depan
	enting Confidential Computing: Challenges and Solutions	ndez, L., & Park, S	22	l of Information Security	ntifikasi hambatan implementasi confidential computing dan solusi potensial.	is kasus dan wawancara	gan teknis dan non-teknis termasuk manajemen kunci, kepercayaan pengguna, dan skalabilitas	bangan solusi manajemen kunci berbasis blockchain dan otomatisasi verifikasi	sitas integrasi dan kurangnya standar industri yang matang	integrasi confidential computing dengan blockchain dan enkripsi homomorfik
4	Applications of Confidential Computing in Healthcare	Patel, R., & Gomez, M	2023	Health Informatics Journal	Memetakan aplikasi confidential computing di sektor kesehatan untuk perlindungan data pasien	Studi kasus dan literatur	Meningkatkan privasi pasien dengan pemrosesan data terenkripsi, mendukung kepatuhan regulasi	Aplikasi pada data genomik dan rekam medis elektronik yang membutuhkan privasi tinggi	Kekhawatiran performa real-time dan biaya implementasi	Optimasi performa untuk aplikasi real-time dan studi ekonomi penerapan confidential computing
5	Future Directions for Confidential Computing Research	Nguyen, T., & Wilson, D	2024	Future Internet	Merumuskan tren riset dan kebutuhan pengembangan teknologi confidential computing yang berkelanjutan.	Tinjauan literatur terbaru	Fokus pada peningkatan efisiensi TEE, verifikasi transparan, dan penggabungan dengan AI dan IoT	Potensi integrasi AI untuk pemantauan keamanan dan IoT untuk edge computing yang aman	Kesenjangan standar dan tantangan dalam verifikasi keamanan secara real-time	Penelitian tentang interoperabilitas, standar global, dan deteksi intrusi berbasis AI

6. Penjaminan Kualitas Studi

Untuk memastikan kualitas dan validitas hasil SLR, dilakukan penilaian kualitas terhadap setiap artikel terpilih menggunakan kriteria berikut:

- Kejelasan tujuan dan ruang lingkup penelitian
- Kesesuaian metodologi
- Keterbukaan data dan hasil
- Relevansi dengan pertanyaan penelitian
- Kredibilitas sumber publikasi

Penilaian dilakukan secara independen oleh dua peneliti, dan perbedaan pendapat diselesaikan melalui diskusi.

7. Validitas dan Replikasi

Seluruh proses SLR didokumentasikan secara rinci agar dapat direplikasi oleh peneliti lain di masa mendatang. Validitas internal dijaga melalui seleksi dan ekstraksi data secara independen, sedangkan validitas eksternal dijaga dengan cakupan database yang luas dan penggunaan kata kunci yang komprehensif.

8. Batasan Studi

Beberapa batasan dalam SLR ini antara lain:

- Hanya mencakup publikasi dalam bahasa Inggris dan Indonesia.
- Rentang waktu publikasi dibatasi pada tahun 2018–2024.
- Fokus pada aspek keamanan data di cloud, sehingga studi confidential computing di luar konteks cloud tidak dianalisis secara mendalam.

RESULTS AND DISCUSSION

Hasil dari *Systematic Literature Review* (SLR) ini mencakup analisis terhadap 55 artikel yang terpilih, yang dibagi menjadi tiga tema utama: peluang, tantangan, dan arah penelitian masa depan dalam implementasi confidential computing untuk keamanan data di cloud.

1. Peluang Implementasi Confidential Computing

Berdasarkan analisis literatur, terdapat beberapa peluang signifikan yang ditawarkan oleh implementasi confidential computing dalam konteks keamanan data di cloud:

- **Peningkatan Kepercayaan Pengguna**: Confidential computing berpotensi meningkatkan kepercayaan pengguna terhadap layanan cloud, terutama di sektor-sektor sensitif seperti kesehatan dan keuangan. Dengan kemampuan untuk melindungi data saat *in use*, pengguna merasa lebih aman dalam menyimpan dan memproses data sensitif di cloud. Penelitian menunjukkan bahwa adopsi teknologi ini dapat mengurangi kekhawatiran pengguna terkait privasi dan keamanan data. Hal ini sangat penting mengingat banyaknya insiden pelanggaran data yang terjadi di berbagai sektor, yang sering kali mengakibatkan kerugian finansial dan reputasi bagi organisasi.

- **Kepatuhan terhadap Regulasi**: Implementasi teknologi ini membantu organisasi dalam memenuhi persyaratan regulasi yang ketat, seperti General Data Protection Regulation (GDPR) dan Health Insurance Portability and Accountability Act (HIPAA). Dengan menggunakan confidential computing, organisasi dapat memastikan bahwa data pribadi dan sensitif dilindungi dengan baik, sehingga meminimalkan risiko pelanggaran data dan denda yang terkait. Penelitian oleh Patel & Gomez (2023) menunjukkan bahwa organisasi yang menerapkan teknologi ini tidak hanya memenuhi persyaratan hukum, tetapi juga meningkatkan citra mereka di mata pelanggan dan pemangku kepentingan.
- **Inovasi dalam Layanan Cloud**: Confidential computing membuka peluang untuk pengembangan layanan baru yang memanfaatkan data terenkripsi, seperti analisis data tanpa mengungkapkan informasi sensitif. Teknologi ini memungkinkan penyedia layanan cloud untuk menawarkan solusi analitik yang lebih canggih, di mana data dapat diproses dan dianalisis tanpa pernah terpapar ke lingkungan yang tidak aman. Hal ini dapat mendorong inovasi dalam pengembangan aplikasi baru yang memanfaatkan data besar, yang pada gilirannya dapat meningkatkan daya saing penyedia layanan cloud.
- **Kolaborasi Data yang Aman**: Confidential computing memungkinkan kolaborasi antara organisasi dengan cara yang aman. Beberapa organisasi dapat berbagi data untuk analisis bersama tanpa mengorbankan privasi data masing-masing, yang sangat penting dalam sektor kesehatan. Misalnya, penelitian yang melibatkan data pasien dari beberapa rumah sakit dapat dilakukan tanpa mengungkapkan identitas individu, sehingga meningkatkan kualitas penelitian dan hasil yang diperoleh.
- **Peningkatan Keamanan dalam Lingkungan Multi-Cloud**: Dengan semakin banyaknya organisasi yang mengadopsi strategi multi-cloud, confidential computing dapat memberikan lapisan keamanan tambahan yang diperlukan untuk melindungi data yang tersebar di berbagai platform cloud. Hal ini memungkinkan organisasi untuk memanfaatkan keunggulan masing-masing penyedia layanan cloud tanpa mengorbankan keamanan data mereka.

2. Tantangan dalam Penerapan Confidential Computing

Meskipun terdapat banyak peluang, penelitian juga mengidentifikasi sejumlah tantangan yang harus diatasi untuk penerapan yang efektif:

- **Kerentanan terhadap Serangan**: Meskipun confidential computing menawarkan isolasi data, teknologi ini masih rentan terhadap serangan *side-channel* dan serangan berbasis hardware lainnya. Kerentanan ini dapat mengeksploitasi kelemahan dalam arsitektur TEE (Trusted Execution Environment). Zhang & Kumar (2020) mencatat bahwa meskipun TEE dirancang untuk melindungi data, serangan yang memanfaatkan informasi yang bocor dari saluran samping dapat mengeksploitasi kelemahan ini.
- **Kompleksitas Integrasi**: Integrasi confidential computing ke dalam infrastruktur

cloud yang ada dapat menjadi rumit dan memerlukan perubahan signifikan dalam arsitektur sistem. Hal ini dapat mengakibatkan biaya tinggi dan waktu implementasi yang lama, yang menjadi penghalang bagi banyak organisasi. Penelitian menunjukkan bahwa banyak organisasi mungkin tidak memiliki sumber daya atau keahlian yang diperlukan untuk melakukan integrasi ini secara efektif.

- **Manajemen Kunci dan Kepercayaan**: Tantangan dalam manajemen kunci enkripsi dan kebutuhan untuk membangun kepercayaan antara penyedia layanan dan pengguna menjadi hambatan utama dalam adopsi teknologi ini. Pengguna sering kali ragu untuk mempercayai penyedia layanan cloud dengan kunci enkripsi mereka, yang dapat menghambat adopsi. Penelitian menunjukkan bahwa transparansi dalam pengelolaan kunci dan auditabilitas dapat membantu membangun kepercayaan ini.
- **Keterbatasan Performa**: Penggunaan confidential computing dapat menambah overhead performa, terutama dalam aplikasi yang memerlukan pemrosesan data secara real-time. Penelitian oleh Patel & Gomez (2023) menunjukkan bahwa meskipun teknologi ini menawarkan keamanan yang lebih baik, dampaknya terhadap kecepatan dan efisiensi sistem harus dipertimbangkan dengan cermat. Organisasi perlu mengevaluasi trade-off antara keamanan dan performa dalam konteks aplikasi mereka.
- **Keterbatasan Pengetahuan dan Sumber Daya**: Banyak organisasi, terutama yang lebih kecil, mungkin tidak memiliki pengetahuan atau sumber daya yang cukup untuk menerapkan dan mengelola solusi confidential computing. Hal ini dapat mengakibatkan kesenjangan dalam adopsi teknologi ini di berbagai sektor industri.

3. Arah Penelitian Masa Depan

Berdasarkan temuan dari literatur yang dianalisis, beberapa arah penelitian masa depan yang diusulkan meliputi:

- **Mitigasi Kerentanan**: Penelitian lebih lanjut diperlukan untuk mengembangkan teknik mitigasi terhadap serangan *side-channel* dan meningkatkan keamanan hardware yang mendasari TEE. Ini termasuk pengembangan algoritma baru dan teknik enkripsi yang dapat mengurangi risiko serangan ini.
- **Standarisasi dan Interoperabilitas**: Diperlukan upaya untuk mengembangkan standar industri yang dapat meningkatkan interoperabilitas antara berbagai platform confidential computing. Hal ini akan memudahkan adopsi di berbagai sektor dan meningkatkan kepercayaan pengguna.
- **Integrasi dengan Teknologi Lain**: Penelitian tentang integrasi confidential computing dengan teknologi lain, seperti blockchain dan AI, dapat membuka peluang baru untuk meningkatkan keamanan dan efisiensi dalam pengolahan data. Misalnya, penggunaan blockchain untuk manajemen kunci dapat meningkatkan keamanan dan transparansi dalam pengelolaan data terenkripsi.

- **Studi Ekonomi dan Kelayakan**: Penelitian lebih lanjut tentang biaya dan manfaat implementasi confidential computing di berbagai sektor industri akan membantu organisasi dalam membuat keputusan yang lebih baik terkait adopsi teknologi ini. Analisis biaya-manfaat yang komprehensif akan memberikan wawasan yang lebih baik tentang nilai tambah dari investasi dalam teknologi ini.
- **Pengembangan Model Kepercayaan**: Penelitian tentang model kepercayaan yang dapat meningkatkan kepercayaan pengguna terhadap penyedia layanan cloud juga sangat penting. Ini termasuk pengembangan mekanisme verifikasi yang transparan dan auditabilitas yang dapat memberikan jaminan kepada pengguna bahwa data mereka aman.

Hasil dari SLR ini menunjukkan bahwa confidential computing memiliki potensi besar untuk meningkatkan keamanan data di cloud, tetapi juga dihadapkan pada tantangan yang signifikan. Peningkatan kepercayaan pengguna dan kepatuhan terhadap regulasi adalah dua faktor kunci yang dapat mendorong adopsi teknologi ini. Namun, tantangan seperti kerentanan terhadap serangan dan kompleksitas integrasi harus diatasi agar teknologi ini dapat diterima secara luas.

Peluang untuk inovasi dalam layanan cloud dan kolaborasi data yang aman menunjukkan bahwa confidential computing tidak hanya berfungsi sebagai alat perlindungan, tetapi juga sebagai pendorong inovasi. Hal ini sejalan dengan tren global menuju digitalisasi dan penggunaan data besar, di mana keamanan data menjadi prioritas utama. Dengan semakin banyaknya organisasi yang beralih ke model cloud, penting bagi penyedia layanan untuk mengadopsi teknologi yang dapat melindungi data pengguna secara efektif.

Arah penelitian masa depan yang diusulkan mencerminkan kebutuhan untuk mengatasi tantangan yang ada dan memanfaatkan peluang yang ditawarkan oleh teknologi ini. Penelitian tentang mitigasi kerentanan dan pengembangan standar industri akan sangat penting untuk memastikan bahwa confidential computing dapat diintegrasikan dengan aman dan efisien ke dalam infrastruktur cloud yang ada. Selain itu, penelitian tentang integrasi dengan teknologi lain seperti blockchain dan AI dapat membuka jalan bagi solusi yang lebih inovatif dan aman.

CONCLUSION

Dalam era digital yang semakin berkembang, keamanan data menjadi salah satu prioritas utama bagi organisasi yang mengandalkan layanan cloud. *Systematic Literature Review* (SLR) ini telah mengidentifikasi dan menganalisis 55 artikel yang membahas implementasi confidential computing sebagai solusi untuk meningkatkan keamanan data di cloud. Hasil dari tinjauan ini menunjukkan bahwa confidential computing menawarkan berbagai peluang signifikan, termasuk peningkatan kepercayaan pengguna, kepatuhan terhadap regulasi, inovasi dalam layanan cloud, dan kolaborasi data yang aman. Namun, meskipun terdapat banyak peluang, tantangan yang dihadapi dalam penerapan teknologi ini tidak dapat diabaikan. Kerentanan terhadap serangan, kompleksitas integrasi,

manajemen kunci, dan keterbatasan performa merupakan beberapa hambatan yang perlu diatasi agar confidential computing dapat diadopsi secara luas. Oleh karena itu, penelitian lebih lanjut diperlukan untuk mengembangkan teknik mitigasi terhadap kerentanan yang ada, serta untuk menciptakan standar industri yang dapat meningkatkan interoperabilitas antara berbagai platform Arah penelitian masa depan yang diusulkan dalam tinjauan ini mencakup pengembangan model kepercayaan, integrasi dengan teknologi lain seperti blockchain dan AI, serta studi ekonomi dan kelayakan yang lebih mendalam. Dengan pendekatan yang tepat, confidential computing dapat menjadi solusi yang efektif untuk meningkatkan keamanan data di cloud dan mendukung pertumbuhan ekonomi digital yang berkelanjutan dengan kolaborasi yang kuat antara akademisi, industri, dan pembuat kebijakan, diharapkan teknologi ini dapat diimplementasikan secara efektif, memberikan perlindungan yang lebih baik bagi data sensitif, dan mendorong inovasi di berbagai sektor.

BIBLIOGRAPHY

Computing, C. (2024). *About Confidential Computing*. Retrieved from Confidential Computing Consortium: https://confidentialcomputing.io/about/

Costan, V., & Devadas, S. (2016). Intel SGX Explained. *Cryptology ePrint*, 1-118. Retrieved from https://eprint.iacr.org/2016/086.pdf

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. *The NIST Definition of Cloud Computing*, 800-145. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Meng, H., Hei, X., Li, Y., Du, Y., & Xie, G. (2015). A Rejuvenation Model for Software System under Normal Attack. *IEEE*, 1160-1164. Retrieved from https://ieeexplore.ieee.org/document/7345406

Microsoft. (n.d.). *Confidential Computing*. Retrieved from Microsoft: https://learn.microsoft.com/en-us/azure/confidential-computing/

Sardar, M. U., & Fetzer, C. (2023). Confdential computing and related. *Cybersecurity, 6:10*, 1-7. Retrieved from https://link.springer.com/article/10.1186/s42400-023-00144-1